iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42265

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Understanding In-Depth About Data Centre Security: Core Concepts & Market Growth

Rishabh Sinha
Digital Content Specialist, Marketing Department, ESDS Software Solution Ltd., Nashik

Abstract: ***Enterprises often perceive Data Centers as a key resource and demand dedicated security initiatives. Further, the emergence of security of the Data Center is playing a critical role in security-critical applications and data in a virtualized environment through optimal safeguarding. The providers of the Data Center have increased their focus. They have shown their participation in the market by enhancing products to augment the increasing demand for Data Center security solutions to address the rising needs of growing industries. This paper discusses various concepts of Data Center security along with its projected market growth on a global level.***

Keywords: Data Centers, Data Center Security, Data Center Security Importance, Data Center Security Market Growth, Data Center Security Practices

I. INTRODUCTION

Cloud Computing and Advanced Technologies have played a major role in transforming how the data is collected, processed, and stored. Enterprises are now migrating their infrastructure to the Cloud, moving their information into safe and encrypted Data Centers backed with multiple security layers. Data Centers keeping sensitive applications and content must be secured physically and virtually in both formats. For a Data Center provider, security needs to be considered with many components, with the major one being adhering to preset compliances and standards.

II. WHY DOES A BUSINESS NEED DATA CENTERS?

For any modern-day enterprise, Data Centers 'virtually' serve as the heart and soul of the core IT operations. Data Centers support a wide array of enterprise activities, including communications and file sharing, processing of data sets, and storing computing resources. In order to perform business tasks and functions, Data Centers demand to have robust computing hardware along with powerful networking equipment. This helps enterprises to process large datasets with ease and via seamless collaborations. Hence, the security of the Data Center becomes inevitable for an organization's operations, productivity & reputation.

III.ESSENTIAL COMPONENTS OF DATA CENTERS

Any Data Center infrastructure usually comprises hardware like routers, switches, firewalls & servers. As the Data Centers offer protection against all forms of threats & malware through restricted access, they must have a robust Data Center ecosystem. A fortified Data Center usually includes the following-

1) *Networking Infrastructure:* Comprising of physical & virtual servers, storage devices, Data Center services along with connectivity to the end-users of Data Centers
2) *Storage Infrastructure:* This includes systems offering secure protection to user data and applications
3) *Computing Resources:* This includes computing resources, including servers, memory, processing, storage, along with local connectivity

All of the components demand power sources, unhindered power supplies, backup generators, cooling systems, fire-fighting equipment as well as secured connection to external networks

IV. UNDERSTANDING DATA CENTER SECURITY

A Data Center depicts a space or facility dedicated to storing an enterprise's IT infrastructure, applications, and critical data. These facilities offer many services like organizing, processing, and storing data, data recovery & backup, and a few others. Data Center security is quite a broad term and includes aspects like practices, policies, and technologies for ensuring the overall protection (virtual & physical) of the Data Center facility. The deployed security measures also need to safeguard the Data Centers from internal and external threats.

Attacks such as data losses, data modification, DDoS attacks, SQL injection attacks, or even theft of intellectual property cause a denting image to the reputation of Data Center providers. To enhance the effectiveness of a Data Center, the Data Center provider must consider some of the following essential parameters-

1) Physical security of the Data Center infrastructure
2) Managing and restricting unprivileged user access
3) Defining security protocols and procedures that have been tested multiple times

It is worth noting that these components are quite complex and constitute different elements; when combined, they effectiveness for Data Center users. All the levels present with the Data Center security must offer work in close coordination to complement the effectiveness of each available security component. The Data Center providers must also ensure that security mechanisms are tested & updated at regular intervals with the end goal of maximum security in the modern day's changing security dynamics.

V. COMMON DATA CENTER VULNERABILITIES

Cybercriminals often use different techniques and tools to get into the Data Centers as well as the security systems residing on these premises. These attack a particular group of users through social engineering attacks to trap the end-users and provoke them to share login credentials or any critical data to intrude into Data Center's security systems. Downloading malware can bring additional risks, allowing cybercriminals to access user data illegally. The use of ransomware has gained significant momentum as attackers "capture and control" user systems, forcing them to pay the ransom to regain system access.

Weak passwords also serve as the soft target for cybercriminals, which are formed as a result of users reusing or recycling their older passwords across their other accounts. Users must understand using the same passwords on different accounts makes it a weak password as they can be easily guessed. Attackers can break through the user's password in different applications since it is used to access resources within the Data Center. This lays the foundation for implementing techniques like Multi-Factor Authentication (MFA) involving at least one thing of the user's concern & one thing that's known.

Additionally, the vulnerabilities within Data Centers can also emerge from incorrectly configured networks or even outdated & legacy security tools. With cybercriminals constantly looking to devise new techniques, Data Center providers must keep the infrastructure equipped with all the required security protocols & tools. Automatic upgradation of software becomes necessary as it uses threat intelligence by putting the Data Center a step ahead against the common online threat vectors.

VI. SECURITY LEVELS OF DIGITAL DATA

Talking about the physical control along with the supporting hardware, they are just a single aspect related to Data Centers. Data Center providers must also follow certain industry-set leading practices for protecting the digital layer of the Data Center from any form of attack. Some of these practices include-

1) Deployment of an intrusion detection system secures the Data Center against advanced threats. To make this detection system effective, continuous monitoring in real-time is required to identify any abnormalities. Common abnormalities include more number of service requests, mismanagement of large data sets, irregular movement of huge chunks of information from the network, or even an increased number of privileged accesses
2) A Building Management System (BMS) is popular technology, with most of the Data Center providers often finding it useful for providing best practices to Data Centers. These systems are complex and responsible for managing various facets involved in running an infrastructure via fire alarms, ventilation areas, climate controls, etc.
3) Using advanced protection levels to secure the network, right from the ground level to encryptions at the network level. It also involves monitoring and performance analysis of all traffic taking place through data transfers

VII. TIPS FOR ENHANCING PHYSICAL SECURITY OF DATA CENTERS

A fully functioning Data Center comprises several mobile parts, which can serve as the base for potential cyberattacks. In order to prevent intrusion attacks, the first thing that Data Center hosting providers must look to have a robust physical security plan in place by keeping in mind the following important considerations-

1) *Selecting a Proper Location:* The end-users must carefully evaluate the Data Center's location facility to remain safe in case of a natural disaster like floods, earthquakes, etc. Also, the Data Center providers need to ensure that they have redundant Data Center facilities present in different seismic zones to provide unhindered data recovery

2) *Restricting Physical Entry Points:* Ideally, a Data Center must have two access points, one being the front entrance which remains accessible by Data Center staff. The other one is the backside, where loading of the dock will take place
3) *Monitoring the Movement:* The Data Center staff must have a complete list of everyone who has been given the access and privileges. These privileges must be immediately rolled back in case these are of no use
4) *Using Security Technology Tools:* Data Centers must also look to implement security technology tools such as multi-factor authentication (MFA) and various security checkpoints across the entire Data Center facility. The security staff must also do multiple checkpoints along with surveillance monitoring by the Data Center team

Apart from the above measures, Data Center Security standards include carrying out timely audits, comprising of multiple checks & compliance audits to ensure the lowest levels of external (environmental) risks. The security staff of the Data Center facility must have a well-defined documentation policy in place defining rules, protocols, and possible consequences if they fail to comply with the physical security of Data Center standards.

VIII. DATA CENTER SECURITY MARKET GROWTH

Online research [1] states that the global Data Center Security Market is predicted to witness a growth CAGR of 17.77% and reach $1.86 billion by 2026, rising from $6.96 in 2019.

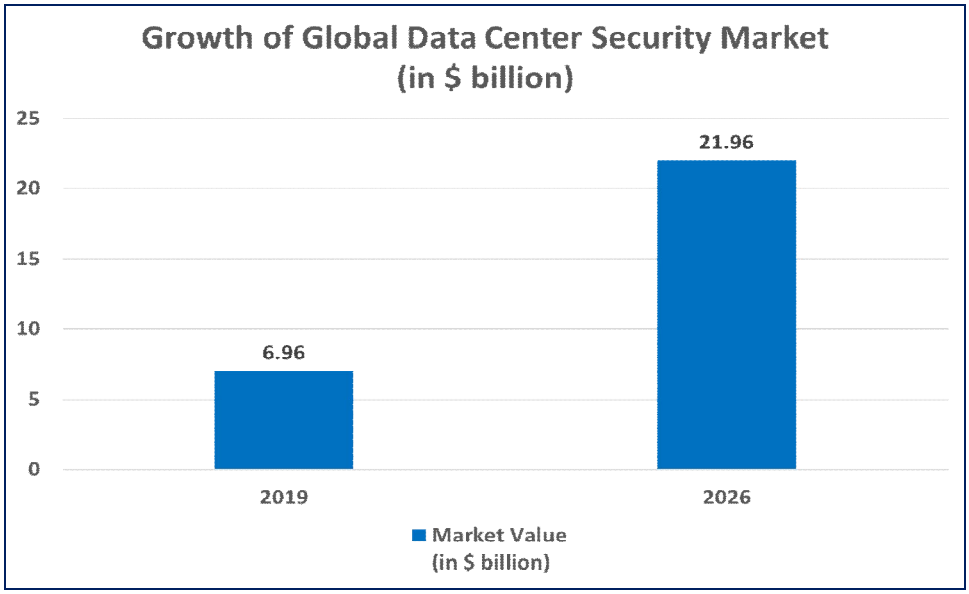


Fig. 1 Graph Depicting Growth of Global Data Center Security Market
Source [1]

The data that end-users generate due to the rising Internet penetration drives the demand for constructing Data Centers to effectively manage, save, and control the data. The largest chunk of Data Center users includes enterprises and hyperscale Cloud Companies optimizing their Data Centers globally. Increasing demand for Data Center security solutions has various concerns associated with the management of Data Centers, which often leads to destruction, loss, and hacking of data causing substantial market growth during the forecasted period. Additionally, there is also an increase in cybercrimes and cyberattacks with the intent to steal data and misuse the same.

A. Market Growth Drivers

The rising demand for advanced security solutions by aiding enterprises in addressing their regulatory compliances is a prominent factor driving this market's growth. Other factors include the adoption of virtualization & Cloud Computing, growth in the number of complex-natured cyberattacks & rise in data traffic, and the immediate need for secured connectivity. Data Center monitoring solutions and capabilities have also been one of the contributing factors enabling the growth of this market. This market segment also offers opportunities like the integration of physical and logical security solutions.

IX. IMPACT OF COVID-19 PANDEMIC ON INDIAN DATA CENTER INDUSTRY

During the pandemic, there was exponential growth due to unforeseen threats that dented the business infrastructure and system. The COVID-19 pandemic caused an accelerated usage of data because the increasing number of users resulted in a demand for bandwidth and storage capacities. In India, the Government of India has undertaken initiatives like Digital India, which heavily emphasizes self-reliance and data protection by data localization, increasing the volume of data, leading to a rise in demand for Cloud and Data Center services. Further, the Government looks to develop the Data Center policy, allowing the private sector players to set up Data Center parks within the country through incentive schemes.

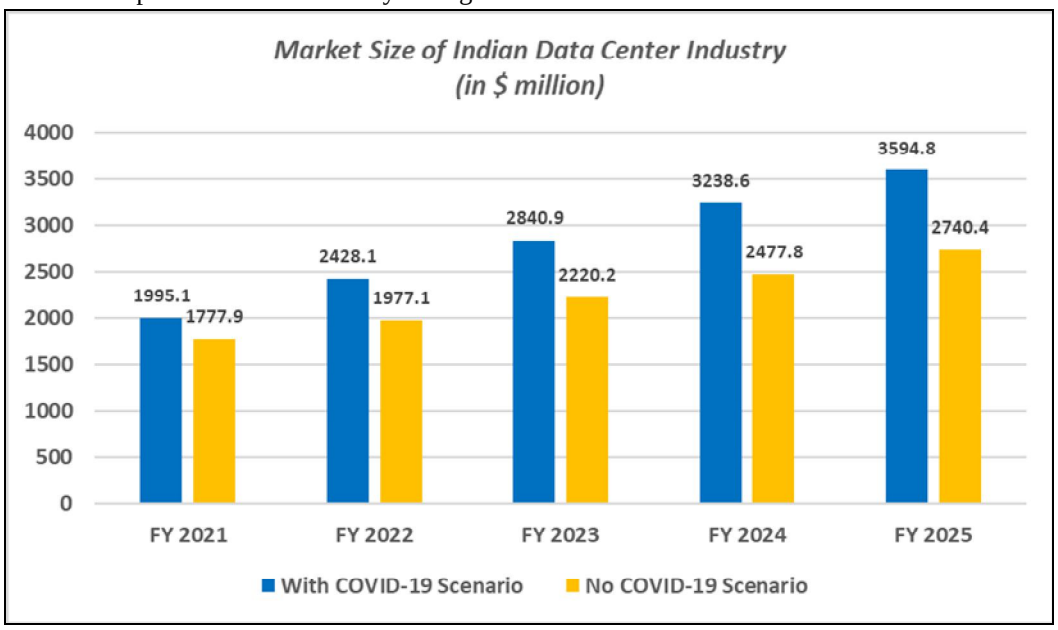


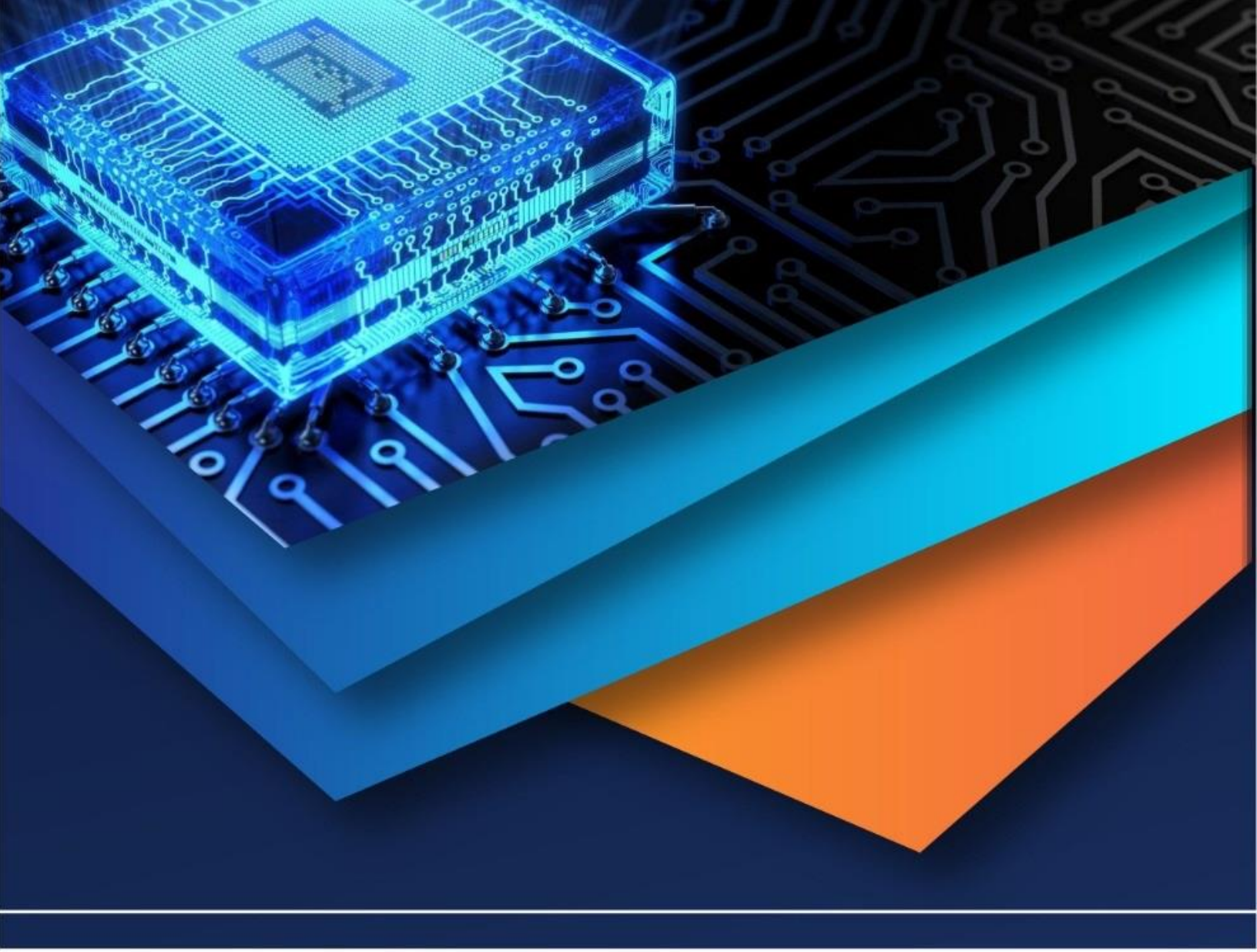
Fig. 2 Graph Depicting Market Size of India (With v/s Without COVID-19 Scenario)
Source [2]

X. CONCLUSION

Data Center providers need to have a comprehensive physical security policy in place. These policies ensure that users having access to critical data and equipment adhere to a defined standard procedure for mitigating risks associated with data breaches and damages related to hardware. Hence, Data Centers have an important role in an enterprise's operations and productivity. Data Centers are expensive investments that store equipment and hardware and host sensitive data and applications. Data Center security can be a complex task, though it is necessary to ensure seamless, safe operations for an organization.

REFERENCES

[1] Data Center Security Market - Forecasts from 2021 to 2026: https://www.researchandmarkets.com/reports/5318003/data-center-security-market-forecasts-from-2021
[2] Interview with Industry Experts and Ken Research Analysis



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY